UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA NORTHEASTERN DIVISION

WILLIAM GRICE	**)**	
	)	
Plaintiff,	**)**	
	)	
v.	**)**	
	)	**Civil Action No.: _________________**
UBER TECHNOLOGIES, INC.,	**)**	**CLASS ACTION**
	)	
Defendant.	**)**	
	)	
	)	
	)	

COMPLAINT

COMES NOW, William Grice, Plaintiff in the above-styled action, files his Complaint both individually and on behalf of a class of similarly-situated individuals against the Defendant Uber Technologies, Inc. (hereinafter, "Uber"), and, in support thereof, show as follows:

INTRODUCTION

1. Plaintiff files this Complaint as a national class action on behalf of over 57 million consumers across the country harmed by Uber's failure to secure and safeguard consumers' Personally Identifiable Information ("PII") which Uber collected from various sources in connection with the operation of its business as a ridesharing mobile application, and for failing to provide timely, accurate and

adequate notice to Consumer Plaintiff and other Class members that their information had been stolen and precisely what types of information were stolen.

2. Uber has acknowledged that a cybersecurity incident ("Data Breach") occurred, potentially impacting approximately 57 million U.S. consumers. It has acknowledged that unauthorized persons stole data about the company's riders and drivers from a third-party server. Uber claims that based on its investigation, the unauthorized access occurred in October of 2016. The information accessed primarily includes names, phone numbers, and email addresses of riders, as well as names and driver's license numbers of about 600,000 drivers in the United States.

PARTIES

3. William Grice is above the age of nineteen (19) and is a resident of Huntsville, Alabama.

4. Uber is a multi-billion-dollar California corporation that provides ridesharing services to millions of consumers across the globe. It enables users to arrange and schedule transportation and/or logistics services with third-party providers.

JURISDICTION AND VENUE

5. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from one defendant, there are more than 100

Class members, and the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs.

6. This Court has personal jurisdiction over Defendant because it conducts business in Alabama and has sufficient minimum contacts with Alabama.

7. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred and/or emanated from this District, and because Defendant has caused harm to Class members residing in this District.

FACTUAL ALLEGATIONS

8. Throughout the past year, Uber collected and stored personal information from Plaintiff, including his name, phone number and email address.

9. Uber owed a legal duty to consumers like Plaintiff to use reasonable care to protect his personal information from unauthorized access by third parties. Uber knew that its failure to protect Plaintiff's personal information from unauthorized access would cause serious risks of harm and identify theft for years to come.

10. On October 21, 2017, Uber announced for the first time that in October of 2016, its database storing Plaintiff's personal information had been hacked by unauthorized third parties, subjecting Plaintiff to credit harm and identify theft.

11. Uber also confirmed that it had paid the unauthorized persons

$100,000.00 to delete the data and keep the Data Breach quiet.

12. Uber executives also made it appear as if the payout had been part of a "bug bounty" – a common practice among technology companies in which they pay hackers to attack their software to test for weaknesses.

13. In an attempt to increase profits, Uber negligently failed to maintain adequate technological safeguards to protect Plaintiff's information from unauthorized access by hackers.

14. Uber knew and should have known that failure to maintain adequate technological safeguards would eventually result in a massive data breach.

15. Uber could have and should have substantially increased the amount of money it spent to protect against cyber-attacks but chose not to.

16. Consumers like Plaintiff should not have to bear the expense caused by Uber's negligent failure to safeguard their personal information from cyber-attackers.

17. Plaintiff hopes Uber will use this massive data breach, and his subsequent lawsuit, as a teachable moment to finally adopt adequate safeguards to protect against this type of cyber- attack in the future.

18. The ramifications of Uber's failure to keep Plaintiff's and Class members' data secure are severe.

19. There may be a time lag between when harm occurs versus when it is

discovered, and also between when personally identifying information is stolen and when it is used.

20. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[1]

21. The PII of Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by Uber. Uber did not obtain Plaintiff and Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

22. The Uber Data Breach was a direct and proximate result of Uber's failure to properly safeguard and protect Plaintiff' and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulation, industry practices, and the common law, including Uber's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff' and Class members' PII to protect against reasonably foreseeable threats to the security or

[1] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 10, 2017).

integrity of such information.

23. Uber had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

24. Had Uber remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Uber would have prevented the Data Breach and, ultimately, the theft of its customers' PII.

25. Plaintiff seeks relief on behalf of himself and as a representative of all others who are similarly situated. Pursuant to FED. R. CIV. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Uber in November 2017 (the "Nationwide Class"). Further, State Subclasses are defined below.

26. Excluded from each of the above Classes are Uber and any of its affiliates, parents or subsidiaries; all employees of Uber; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

27. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

28. Each of the proposed Classes meets the criteria for certification under FED. R. CIV. P. 23(a), (b)(2), (b)(3) and (c)(4).

29. **Numerosity. FED. R. CIV. P. 23(a)(1).** Consistent with RULE 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, the proposed Class include at least 57 million individuals whose PII was compromised in the Uber Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

30. **Commonality. FED R. CIV. P. 23(a)(2) and (b)(3).** Consistent with FED. R. CIV. P. 23(2)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a) Whether Uber had a duty to protect PII;

b) Whether Uber knew or should have known of the susceptibility of their data security systems to a data breach;

c) Whether Uber's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;

d) Whether Uber was negligent in failing to implement reasonable and adequate security procedures and practices;

e) Whether Uber's failure to implement adequate data security measures allowed the breach to occur.

f) Whether Uber's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of PII of Plaintiff and Class members;

g) Whether Plaintiff and Class members were injured and suffered damages or other acceptable losses because of Uber's failure to reasonably protect its systems and data network; and

h) Whether Plaintiff and Class members are entitled to relief.

31. **Typicality. FED. R. CIV. P. 23(a)(3).** Consistent with FED. R. CIV. P. 23(a)(3), Plaintiff's claims are typical of those of other class members. Plaintiff had his PII compromised in the Data Breach. Plaintiff's damages and injuries are akin to other Class members and Plaintiff seeks relief consistent with the relief of the Class.

32. **Adequacy. FED. R. CIV. P. 23(a)(4).** Consistent with FED. R. CIV. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Uber to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class.

Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

33. **Superiority. FED. R. CIV. P. 23(b)(3).** Consistent with FED. R. CIV. P. 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiff may not be sufficient to justify individual litigation. Here the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Uber, and thus, individual litigation to redress Uber's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

34. **Injunctive and Declaratory Relief.** Class certification is also appropriate under FED. R. CIV. P. 23(b)(2) and (c). Defendant, through its uniform

conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

35. Likewise, particular issues under RULE 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a) Whether Uber failed to timely notify the public of the Breach;

b) Whether Uber owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c) Whether Uber's security measures were reasonable in light of data security recommendation, and other measures recommended by data security experts;

d) Whether Uber failed to adequately comply with industry standards amounting to negligence;

e) Whether Defendant failed to take commercially reasonable steps to safeguard the PII of Plaintiff and the Class members; and

f) Whether adherence to data security recommendations and measures recommended by data security experts would have reasonably prevented the Data Breach.

36. Finally, all members of the proposed Classes are readily ascertainable.

Uber has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for the purposes of providing notice to the Class.

CAUSES OF ACTION

Count I
Negligence
(On behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Separate Statewide Classes)

37. Plaintiff restates and reallege Paragraphs 1 through 36 as if fully set forth herein.

38. Upon accepting and storing the PII of Plaintiff and Class Members in its computer systems and on its networks, Uber undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Uber knew that the PII was private and confidential and should be protected as private and confidential.

39. Uber owed a duty of care not to subject Plaintiff and Class members, along with their PII, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

40. Uber owed numerous duties to Plaintiff and to members of the Nationwide Class, including the following:

a) To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b) To protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c) To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

41. Uber also breached its duty to Plaintiff and the Class members to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Uber failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted and unknown third party to gather PII of Plaintiff and Class members, misuse the PII and intentionally disclose it to others without consent.

42. Uber knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Uber knew about numerous, well-publicized data breaches, including the breach at Experian.

43. Uber knew, or should have known, that their data systems and

networks did not adequately safeguard Plaintiff' and Class members' PII.

44. Uber breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiff and Class members.

45. As a direct and proximate result of Uber's conduct, Plaintiff and the Class suffered damages, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

Count II
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Separate Statewide Classes)

46. Plaintiff restates and reallege Paragraphs 1 through 36 as if fully set forth herein.

47. Section 5 of the FTC Act prohibits "unfair… practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Uber, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Uber's duty in this regard.

48. Uber violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Uber's conduct was particularly unreasonable given the

foreseeable consequences of a data breach at a corporation such as Uber, including, specifically, the immense damages that would result to Plaintiff and Class members.

49. Uber's violation of Section 5 of the FTC Act constitutes negligence *per se*.

50. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

51. As a direct and proximate result of Uber's negligence per se, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the far-reaching, adverse, and detrimental consequences of identity theft and loss of privacy.

Count III
Declaratory Judgement
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Separate Statewide Classes)

52. Plaintiff restate and reallege Paragraphs 1 through 36 as if fully set forth herein.

53. As previously alleged, Plaintiff and Class members entered into an implied contract that required Uber to provide adequate security for the PII it collected from their transactions. As previously alleged, Uber owes duties of care to Plaintiff and Class members that require it to adequately secure PII.

54. Uber still possesses PII pertaining to Plaintiff and Class members.

55. Uber has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and most importantly, its systems.

56. Accordingly, Uber has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Uber's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

57. Actual harm has arisen in the wake of the Uber Data Breach regarding Uber's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

58. Plaintiff, therefore, seek a declaration that (a) Uber's existing data security measures do not comply with its contractual obligations and duties of care and (b) in order to comply with its contractual obligations and duties of care, Uber must implement and maintain reasonable security measures.

Count IV
Violation of Alabama Deceptive Trade Practices Act
(ALA CODE 1975 § 8-19-1 *et seq*.)

59. Plaintiff restate and reallege Paragraphs 1 through 36 as if fully set forth herein.

60. Plaintiff William Grice brings this claim on behalf of himself and the Alabama Subclass.

61. Defendant's misrepresentations, active concealment, and failures to

disclose violated the Alabama Deceptive Trade Practices Act ("DTPA") in that Defendant misrepresented that its services and products were of a particular standard, quality, and/or grade when they were of another (Ala. Code § 8-19-5(7)).

62. As previously alleged, Plaintiff and Class members entered into an implied contract that required Uber to provide adequate security for the PII it collected from their transactions. As previously alleged, Uber owes duties of care to Plaintiff and Class members that require it to adequately secure PII.

63. The foregoing acts and omissions of the Defendant were undertaken willfully, intentionally, and knowingly as part of its routine business.

64. Defendant's misrepresentations and omissions were material to Plaintiff and members of the Alabama Subclass, such that a reasonable person would consider them important in deciding whether to purchase Defendant's services, and had Plaintiff and members of the Alabama Subclass known the truth, they would have acted differently.

65. The conduct described herein has tremendous potential to be repeated where other consumers similarly-situated will be treated with the same unscrupulous, unethical, unfair and deceptive acts and practices.

66. Furthermore, as alleged above, Uber's failure to secure consumers' PII violates the FTCA and therefore violates the DTPA.

67. Uber knew or should have known that its computer system and data

security practices were inadequate to safeguard the PII of Plaintiff and Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

68. As a direct and proximate result of Uber's violation of the DTPA, Plaintiff and Class members suffered damages which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

69. Also as a direct result of Uber's knowing violation of the DTPA, Plaintiff and Class members are entitled to damages as well as injunctive relief, including, but not limited to:

a) Ordering that Uber engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Uber's systems on a periodic basis, and ordering Uber to promptly correct any problems or issues detected by such third-party security auditors;

b) Ordering that Uber engage third-party security auditors and internal personnel to run automated security monitoring;

c) Ordering that Uber audit, test, and train its security personnel regarding any new or modified procedures;

d) Ordering that Uber segment PII by, among other things, creating firewalls and access controls so that if one area of Uber is compromised, hackers cannot gain access to other portions of Uber systems;

e) Ordering that Uber purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f) Ordering that Uber conduct regular database scanning and securing checks;

g) Ordering that Uber routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h) Ordering Uber to meaningfully educate its customers about the threats they face as a result of the loss of their personal information to third parties, as well as the steps Uber customers must take to protect themselves.

70. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and Class members and the public from Uber's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Uber's wrongful conduct as

alleged in this Complaint has had widespread impact on the public at large.

71. Plaintiff and Class members are entitled to a judgment against Uber for actual and consequential damages, exemplary damages and attorneys' fees pursuant to the DTPA, costs, and such other further relief as the Court deems just and proper.

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Uber as follows:

a) For an Order certifying the Classes, as defined herein, and appointing Plaintiff and their Counsel to represent the Nationwide Class, or in the alternative the separate Statewide Classes;

b) For equitable relief enjoining Uber from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff' and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class members;

c) For equitable relief compelling Uber to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of PII compromised;

d) For an award of damages, as allowed by law in an amount to be determined;

e) For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f) For prejudgment interest on all amounts awarded; and

g) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demand a jury trial on all issues so triable.

Submitted this the 22nd day of November, 2017.

s/ Eric J. Artrip
Eric J. Artrip (ASB-9673-I68E)
D. Anthony Mastando (ASB-0893-X32B)
MASTANDO & ARTRIP, LLC
301 Washington St., Suite 302
Huntsville, Alabama 35801
Phone: (256) 532-2222
Fax: (256) 513-7489
artrip@mastandoartrip.com
tony@mastandoartrip.com

DEFENDANT TO BE SERVED VIA CERTIFIED MAIL

Uber, Inc.
Attn CT Corporation System
2 North Jackson Street, Suite 605
Montgomery, AL 35104